

TRANSMISSION SYSTEM FOR DECODING KEY**Patent number:** JP2041046**Publication date:** 1990-02-09**Inventor:** HIRASHIMA MASAYOSHI**Applicant:** CONDITIONAL ACCESS TECH**Classification:**

- international: H04H1/00; H04L9/06; H04L9/14; H04L9/34;
H04N7/167; H04H1/00; H04L9/06; H04L9/14;
H04L9/34; H04N7/167; (IPC1-7): H04H1/00; H04L9/06;
H04L9/14; H04L9/34; H04N7/167

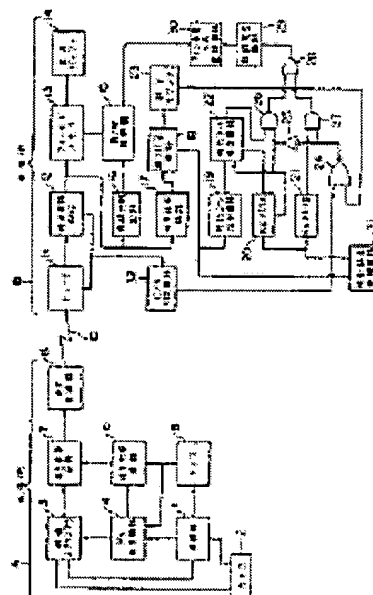
- european:**Application number:** JP19880190599 19880801**Priority number(s):** JP19880190599 19880801**Best Available Copy**

Report a data error here

Abstract of JP2041046

PURPOSE: To attain release of scrambling even if C/N(carrier/noise) is deteriorated by sending a decoding key at a comparatively short time interval and sending plural release keys each intermittently or continuously in relation with time information.

CONSTITUTION: When the C/N reaches a certain value or below, an output of a C/N discrimination circuit 32 goes to a high level. Then an output of an OR gate 24 goes to a low level, an AND gate 27 is cut off and an output of an inverter 25 goes to a high level and an AND gate 26 is conductive. A time code collation circuit 22 starts the collation after an output of the inverter 25 goes to a high level. Then a data Ks20 of a Ks memory A 20 is read and given to a random number generating circuit 29 via the AND gate 26 an OR gate 28 and a conversion circuit 30 converts a generated random number into a line number. Thus, while the decoding key Ks is being switched continuously, descrambling is continued.



Data supplied from the esp@cenet database - Worldwide

⑫ 公開特許公報(A) 平2-41046

⑪ Int. Cl.⁵

識別記号

庁内整理番号

⑬ 公開 平成2年(1990)2月9日

H 04 H 1/00
 H 04 L 9/06
 9/14
 9/34
 H 04 N 7/167

F 7608-5K

8725-5C
 7240-5K
 7240-5K

H 04 L 9/00
 9/02

B
 Z

審査請求 有 請求項の数 3 (全7頁)

⑭ 発明の名称 解読鍵の伝送方式

⑮ 特 願 昭63-190599

⑯ 出 願 昭63(1988)8月1日

⑰ 発 明 者 平 嶋 正 芳 東京都港区虎ノ門1丁目20番7号 株式会社コンディショ
 ナル・アクセス・テクノロジー研究所内

⑱ 出 願 人 株式会社コンディショ 東京都港区虎ノ門1丁目20番7号
 ナル・アクセス・テ
 ク
 ノロジー研究所

⑲ 代 理 人 弁理士 浅 村 皓 外3名

明 細 書

1. 発明の名称

解読鍵の伝送方式

2. 特許請求の範囲

(1) 送信側から受信側へ情報を伝送するに際し、送信側で前記情報を分割しかつ分割された情報の順序を並べ替えると共に、受信側で解読鍵を用いて元の順序に並べ直し前記情報を再現する伝送方式において、前記解読鍵を比較的に短い時間間隔で変化させ、前記時間間隔で1個ずつ伝送すると共に、併せて前記解読鍵を複数個ずつ時刻情報と関連させて間欠的又は連続的に伝送することを特徴とする解読鍵の伝送方式。

(2) 請求項(1)において、複数の前記解読鍵のそれぞれに時刻情報を対応させ、前記時刻情報と前記解読鍵とを一括に伝送することを特徴とする解読鍵の伝送方式。

(3) 請求項(1)又は(2)において、受信側で信号伝送路のC/Nの変化を検出し、前記C/Nの変化に対応して、使用すべき鍵を、個別に伝送される鍵

と時刻情報に対応させてまとめて伝送される鍵とのいずれかに切り替えることを特徴とする解読鍵の伝送方式。

3. 発明の詳細な説明

[産業上の利用分野]

本発明は放送システムにおけるスクランブルを解除するための解読鍵の伝送方式に関する。

[従来の技術]

衛星放送等の有料放送システムでは視聴契約の加入者のみに番組が提供されるように、放送局において番組信号にスクランブルをかけて送信を行う。一方、加入者の側ではスクランブル鍵を用いてスクランブルを解除し番組信号を取り出す。これにより加入者のみの番組視聴を可能にし、不正視聴を防止する。スクランブルされた番組信号をデスクランブルするためのスクランブル鍵は一般に番組信号と同じ伝送路で例えば毎秒ごとに伝送されるが、このような場合、スクランブル鍵の不正解読を防止不正視聴を確実に防止するために、毎秒送られるスクランブル鍵を短時間(例えば

10秒)で変更する。

〔発明が解決しようとする問題点〕

スクランブル鍵を短時間で変更して送る方式では、受信側でスクランブル鍵が送られてくる度に取り出してスクランブルを解除しなければならない。このような場合、例えば、FMを利用する衛星放送において、降雨又はアンテナの向きが狂う等の理由によりC/N(carrierとnoiseとの比)が低下すると、映像、音声、制御信号にノイズが多数入り、スクランブル鍵を正確に取り出すことができなくなる。この結果受信側においてスクランブルの解除が不可能になる。特に、スクランブル鍵を10秒に1回変更するシステムにおいては、スクランブル鍵の受信を1回誤ると10秒の間スクランブルを解除することができないという不具合が生じる。

〔問題点を解決するための手段〕

本発明に係る解読鍵の伝送方式は、送信側で番組等の情報を分割し、分割したものの順序を並べ替えて受信側へ伝送し、受信側で情報と同一伝送

路で伝送されてくる解読鍵を用いて元の順序に並べ直し情報を再現する伝送方式において、前記解読鍵を比較的短い時間間隔で変化させかつこの時間間隔で伝送すると共に、併せて解除鍵を時刻情報と関連させて複数個ずつ間欠的又は連続的に伝送するようにしている。

〔作用〕

受信側では伝送路のC/Nの状態を検出し、C/Nの状態に対応してスクランブル解除するために使用する鍵を決定する。解読鍵を時刻情報に対応させて複数個まとめて伝送するようにしたから、所定時間内で一度でも正しく解読鍵を受信できれば、C/Nが低下した場合でも先に受信した鍵を使用することによつてスクランブル解除を行うことが可能となる。

〔実施例〕

以下に本発明の好適実施例を添付図面に従つて説明する。

第1図は本発明に係る放送システムをブロック図で示したもので、第1図中左側のAは送信側の

回路構成であり、右側のBは多数の受信側の1つを示す回路構成である。この実施例では一例として送信側Aと受信側Bとを結ぶ伝送路10として衛星放送電波を利用している。従つてこの放送システムは衛星を利用した有料放送システムであり、不正視聴を防止する目的で映像信号と音声信号の両方にスクランブルがかけられている。以下の説明では説明の便宜上映像のスクランブルについてのみ説明する。また伝送路10におけるC/N(carrierとnoiseとの比)の劣化は1回につき30秒以内と仮定する。

第1図に示された回路の構成を説明する。

送信側Aにおいて、1は送信側の同期盤、2は信号源としてのカメラ(VTRやディスクでもよい)、3はカメラ2の映像出力にスクランブルをかけるスクランブラー、4はスクランブルをかけるための乱数の基準となる鍵Ksを発生させるKs発生回路であり、同期盤1で同期をとつている。鍵Ksはスクランブルを解除するための解読鍵である。5は同期盤1に同期しているタイマ、

6は第2図のA、Bに示す信号形式で鍵Ksやその他の情報を送出するための信号形成回路、7は第2図A又はBの形式の信号をテレビ信号中のVB I(垂直帰線期間)の1水平走査期間に重畳する重畳回路である。タイマ5はKs発生回路4と信号形成回路6との同期をとつている。8はRF変調器であり、このRF変調器8の出力が衛星を介し、日本全国に散在する多数の受信局の各受信アンテナ(図示せず)へ伝送される。

受信側Bにおいて、受信アンテナから図示しないLNB(Low Noise Block down convertor)を経てチューナ11へRF変調器8の出力が供給される。チューナ11では、受信した信号を選択し、中間周波(例えば約400MHz)に変換し、検波回路12でFM検波する。また検波回路12はAGC電圧も発生し、これをチューナ11へ帰還している。チューナ11と検波回路12は通常のBSチューナの回路と同一である。13は検波回路12の出力信号を2フィールド分ストアするフィールドメモリであり、2つの1フィールドメモ

りから成る。14は出力バツファ、15はフィールドメモリ13の書込みと読み出しを制御するR/W制御器である。16は検波回路12から出力されるテレビ信号から同期信号を分離する同期分離回路、17は上記テレビ信号からVBI中の各種信号を取り出すための信号抜取回路であり、この回路は送信側Aから送られてくる第2図A、Bに示される信号を抜き取り、サンプリングしてデジタル信号に変換する。18は文字放送で使用されているものと同一ないわゆるBEST方式と呼ばれる誤り訂正回路である。誤り訂正回路18の出力信号は、誤りカウンタ23、時刻コード抜取回路19、暗号・課金処理回路31に供給される。暗号・課金処理回路31で得られた情報はKsメモリA20とKsメモリB21に供給され、これらのメモリのそれぞれに記憶される。22は時刻コード照合回路であり、この回路には時刻コード抜取回路19とKsメモリA20の各出力が入力される。また32はC/N判定回路で、検波回路12から出力されるAGC電圧によつてC/Nの

状態を判定する。受信側Bはその他に、NORゲート24、インバータ25、ANDゲート26、27、ORゲート28を含む。NORゲート24はC/N判定回路32と誤りカウンタ23の各出力を入力し、その出力をインバータ25とANDゲート27へ与える。インバータ25はその出力をKsメモリA20と時刻コード照合回路22とANDゲート26に与える。ANDゲート26の残りの入力には時刻コード照合回路22の出力が入力され、またANDゲート27の残りの入力にはKsメモリB21の出力が入力される。ANDゲート26、27の各出力はORゲート28に与えられる。29は乱数発生回路、30はライン番号への変換回路であり、ORゲート28の出力を受けて乱数発生回路29が乱数を発生し、ライン番号への変換回路30を経て前述のR/W制御器15に対して制御用信号を与える。

次に第1図に示された回路の作用について説明する。

送信側Aでの映像信号にスクランブルをかける

動作は映像スクランブラ3において行われる。映像スクランブラ3において、カメラ2から出力された映像信号はKs発生回路4から与えられる鍵Ksによつてスクランブルをかけられる。スクランブルをかけるために使用された鍵Ks及びその他の信号は、信号形成回路6を経て信号重畳回路7に与えられ、この信号重畳回路7で、映像スクランブラ3から供給されるスクランブルをかけられた映像信号のVBIの1水平走査期間の中に重畳され、その後RF変調器8を経て受信側へ送出される。

次に受信側Bにおけるデスクランブル動作を簡単に述べる。KsメモリB21において得られる24ビットの鍵Ksを用いて乱数発生回路29でPN系列($2^{24}-1$)を発生させ、このPN値を用いて変換回路29で予め決めた手順(例えば、8ビットの数をROMで変換する)に従つてライン番号(水平走査線の番号)に変換し、この番号を用いて、フィールドメモリ13の中から正しい順序で信号を読み出し、出力バツファ14を介し

CRT等のディスプレイに元の画面を表示する。かかる動作は、テレビ画面を送信側でスクランブルし、その受信側でデスクランブルする一例であり、特にラインパーミュテーションと呼ばれている。この場合、送信側Aの映像スクランブラ3で使用される乱数、それに基づくライン番号、及びその順序は、受信側の乱数発生回路29と変換回路30で行われる作用と互いに逆(相補関係)になっている。

前記回路の作用を更に詳しく説明する。スクランブルシステムでは鍵Ks以外にも各種情報を送受する必要がある。現在放送されている日本の衛星放送の場合、PCM音声の他にデータも送れる。この実施例では、一般的に適用できる方式としてVBIの1Hを用いる例を考える。毎フィールド1Hを使い、1H中ヘッダーを除く184ビットを制御情報その他に使うものとする。鍵Ksを10秒毎に変更すれば、鍵Ksは10秒に1回送出すればよい。この間のフィールド数は $60 \times 10 = 600$ フィールドであり、残りの599Hを利

用して鍵Ks以外の情報を送ることができる。また毎秒10回余分にKsを送るものとするれば10秒間に $10 \times 10H$ 、すなわち $100H$ を使うことになる。従つて、この場合には $600H$ 中 $101H$ を鍵Ksの伝送に使う。以下においてはこの条件に基づいて説明する。残りの $600 - 101 = 499H$ の各1H当り144ビットを各種制御や端末アクセス等についての制御情報に割当てることができる。

第2図はVBIの1Hに含まれる2種類のデータバケットを示す。Aは鍵Ksの情報を送るデータバケットであり、Bは鍵Ks以外の制御情報を送るデータバケットである。データバケットAでは鍵Ksは24ビットであり、鍵Ksを例えば6個($n=6$)まとめて送るようにしている。またデータバケットA、Bにはそれぞれ6ビットのヘッダーと40ビットの時刻コード等の情報が含まれている。ヘッダーの内容については第3図に示される。

検波回路12で出力されるスクランブルされた

映像信号はフィールド毎にフィールドメモリ13内の第1及び第2の1フィールドメモリにフィールドの順序に従つて交替させて記憶される。R/W制御器15がフィールドメモリ13における書込みと読出しを制御することにより受信側のデスクランブルが行われる。すなわち、R/W制御器15は、第nフィールドのスクランブルされた映像信号を検波回路12からそのままフィールドメモリ13の中の第1の1フィールドメモリに書き込み、この間、第2の1フィールドメモリに書き込まれている第n-1フィールドの映像信号を、変換回路30の指示に従い、CRT等の表示装置上で正常な映像が見えるような順序で走査線単位に読み出す。また、第n+1フィールドの映像信号では、第2の1フィールドメモリへ検波回路12の出力する映像信号をそのまま書き込み、この間第1のフィールドメモリから第nフィールドの映像信号を、変換回路30の指示に従い、CRT等の表示装置上で正常な画が見えるような順序で走査線単位に読み出す。これをフィールド

毎に繰返すことによりデスクランブル動作が継続される。

誤り訂正回路18における誤り訂正は、第2図A、Bの190ビットの部分に対して行われる。この190ビット中の、144ビットは暗号化されている。暗号化部分は暗号・課金処理回路31の暗号処理部で復号され、時刻コードと一緒にKsメモリA20又はKsメモリB21に記憶される。KsメモリB21には現在フィールドメモリ13から読み出すための鍵Ksが記憶され、KsメモリA20には将来のフィールドメモリ13からの読み出しに使う鍵Ksが複数個時刻コードと共に記憶されている。

ここでC/Nが低下して誤りが増加した場合を考える。C/Nが低下すると、検波回路12のAGC電圧が上昇(又は下降)する。C/Nがある値以下になると、C/N判定回路32の出力が高レベルになる。C/N判定回路32の出力が高レベルとなると、ORゲート24の出力が低レベルとなり、ANDゲート27は遮断され、またイ

ンバータ25の出力が高レベルとなつてANDゲート26が導通する。また誤り訂正回路18での誤り訂正の回数が一定値以上になると、誤りカウンタ23から高レベルが出力され、ORゲート24の出力が低レベルとなり、ANDゲート26が導通し、ANDゲート27が遮断される。時刻コード抜取回路19では、第2図Bの形式の制御信号以外の非暗号化部の時刻コード $\times \times$ 分 $\Delta \Delta$ 秒(BCDで $4 \times 4 = 16$ ビット)を受信する。この時刻コードが例えば6フィールド毎に送られているものとする、約0.1秒毎に時刻コードが変化する。一方、KsメモリA20には $\times \times$ 分 $\Delta \Delta$ 秒という時刻コードと共に、第2図Aの鍵Ksが6個入っている。仮に $\Delta \Delta$ 秒として10秒であるとする、10~19秒の時刻コードが送られている間は、第4図に示すKs10~Ks20が、第2図Aの形式で送られており、C/Nが低下しないとき及び誤り訂正の回数が少ないときには、KsメモリA20へは第2図Aの信号を受信する毎にKs10~Ks00の 24×6 ビットを書き込ん

でいる。××分15秒でC/Nが低下し、インバータ25の出力が高レベルになったとすると、それ以降KsメモリA20の書換えは中止される。その時の内容は第4図の通りである。××分15秒の時刻までは正常受信であつたから、KsメモリB21の記憶内容は第4図のKs10と同じである。時刻コード照合回路22はインバータ25の出力が高レベルになった後照合を始める。しかし、C/Nが低下していると、第2図A、Bに示される時刻コードに誤りが含まれていることが多いので、時刻コード照合回路22は内部にタイマを有し、インバータ25の出力が低レベルの間(C/Nが高い時)、時刻コード抜取回路19の出力でタイマを校正する。C/N低下が1日中続くことはない。ここではC/N低下の間を30秒以下と考えているので、その間タイマが進み遅れることはない。従つて、時刻コードは時刻コード照合回路22の中で分秒4桁を形成し、そのコードと第4図の分秒のコードとを比較する。従つて、××分20秒になると、KsメモリA20の中の

××分20秒のデータKs20を読み出し、これをANDゲート26及びORゲート28を経て乱数発生回路29へ伝え、乱数発生回路29でKs20を基にして乱数を発生させ、この乱数から変換回路30でライン番号へ変換する。以上の動作は、C/Nが高い時と同じである。例えば××分44秒にC/Nが高くなつて、C/N判定回路32の出力と誤り訂正カウンタ23の出力の両方が低レベルになると、KsメモリB21の出力(Ks50)がANDゲート27及びORゲート28を介して乱数発生回路29へ××分50秒に伝えられる。××分44秒から××分50秒まではKsメモリA20から読み出されたKs40に基づいて発生した乱数が使われる。××分50秒には、第5図に示されるKs50~Ks40'が送られ、KsメモリA20へ書き込まれる。この場合、KsメモリB21へ書き込まれるKs50を、第2図Bで先に送り、次のフィールドでは第2図Aで送る。必要なら、第2図Bを、××分50秒の寸前(2フィールド以上前)に残いて第2図Aを送るようにして

もよい。このようにすれば、連続して鍵Ksを切り換えつつデスクランブルし続けることができる。なお、鍵Ksを切換時刻よりも先に送る時は、時刻コード照合回路22で、KsメモリB21の内容についても時刻コードの照合を行い、KsメモリB21にも時刻コード付きで鍵Ksを記憶しておけばよい。この場合も、時刻照合はC/N低下時のみ停止させればよい。

以上で本発明の基本的動作の説明はできたが、第3図と共に、第2図について説明を補足する。前述の通り第2図A、Bのヘッダーは6ビットで、例えば第3図の如く $b_0 \sim b_5$ の値と、各パケットの意味を対応させることができる。例えば1分間に使う鍵Ksが6個ではなく、10分間に使う鍵Ksを60個まとめて送ることとし、 $b_0 \sim b_5$ の示す数値1~10を用いて複数の鍵Ksを含むパケット(第2図A)を区別し、第4図、第5図の鍵Ksのメモリ容量を、時刻コードも含めて10倍にすれば、10分以下のC/N低下に対し同様の考え方で処理でき、C/N低下により鍵

Ksを受信できなくなつても10分以内であれば引続きデスクランブルできる。なお、第2図Bの制御情報の中味は、システムに応じて決められる。

第6図は垂直同期間を用いて鍵Ksを送るタイミング例を示す。先の説明では××分45秒を考える。 $B_1 \sim B_n$ は、10秒毎に送る第2図Bの形式の信号の送出時点及び送出間隔を示し、 B_1 と B_2 間は600フィールド離れている。一方 A_1, A_7, \dots は本発明に示されるように鍵Ksをまとめて送る時点を示している。ここでは $B_1 \sim B_n$ と同一フィールドの部分のみ、 A_1, \dots, A_7, \dots を示している。拡大図に示す如く、15H目Ks50を送り、16H目にKs50~Ks40'を送れば、両方を同一フィールドで送ることができる。また10分単位で考えるときは、第7図の如く、1フィールドの11Hを用い、11H目に第2図B、12~21Hに第2図Aを10種類送ればよい。

前記実施例では、ラインバーミュレーションと呼ばれるスクランブル方式で説明したが、本発明

を他のスクランブル方式に適用できるのは勿論である。また、鍵を複数個 (n 個) 送る場合には、間欠的又は連続的にこれを送ることができる。更に本発明の基本思想は、衛星放送以外の種々の有料放送システムに適用することが可能である。

〔発明の効果〕

以上の説明で明らかなように本発明によれば、個別に鍵を伝送するのに併せて、有料放送システムにおいて受信側で使用されるスクランブル解除のための解読鍵を時刻情報に関連させこれと共に所定時間分先に送って記憶させ、通常は時々刻々変化する鍵を使用して、デスクランブルを行い、C/Nが低下したときには先に送られた鍵と時刻を照合し適切な鍵を使用することができるため、受信側でスクランブル解除を中断することがない。

4. 図面の簡単な説明

第 1 図は本発明の一実施例を示す回路構成図、
第 2 図は 2 種類のデータパケットを示す説明図、
第 3 図はヘッダの内容を表で示した説明図、
第 4 図及び第 5 図は時刻と鍵の関係を表で示す

說明圖、

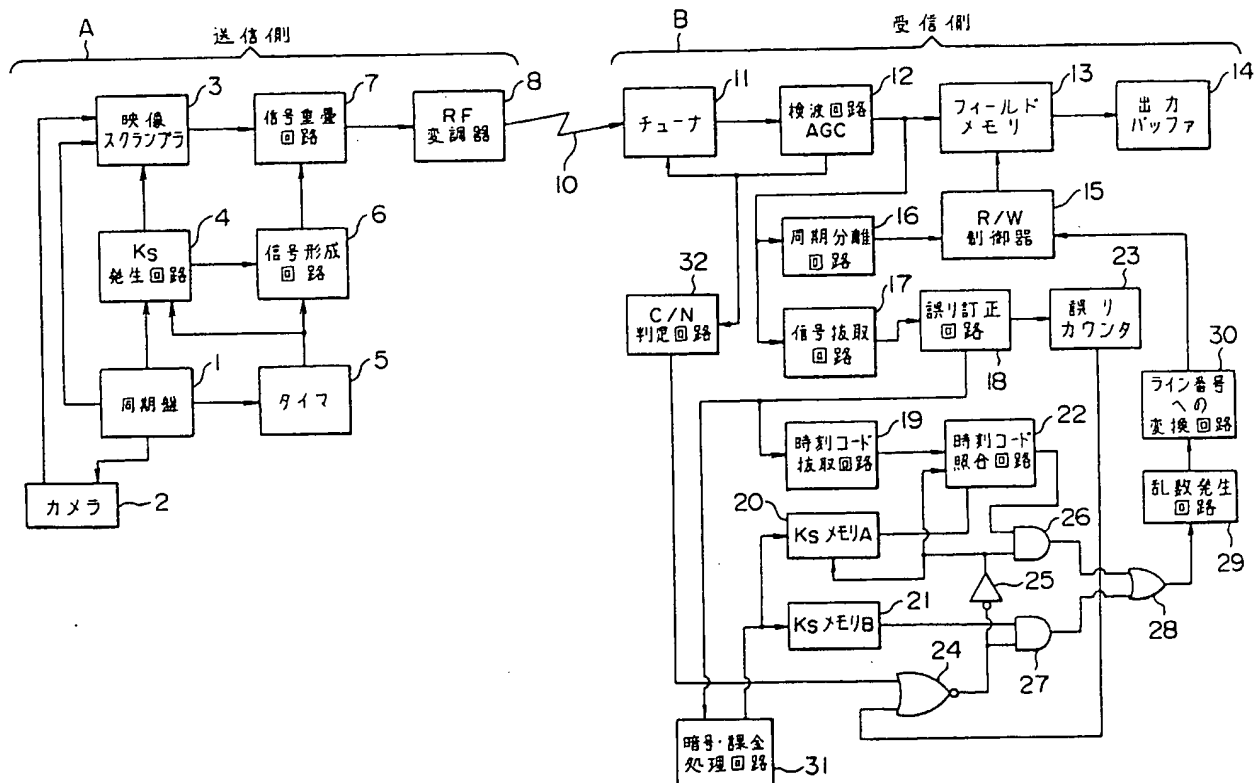
第 6 図及び第 7 図はデータパケットの配設状態を示す説明図である。

[符 号 の 説 明]

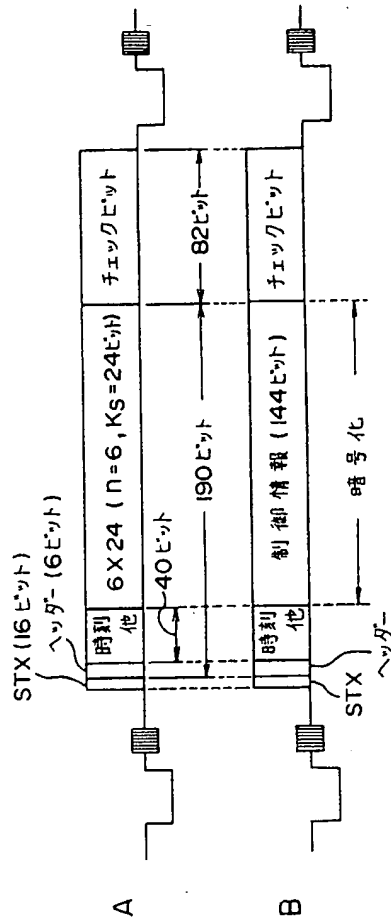
- 3 … 映像スクランブラ
- 4 … K s 発生回路
- 7 … 信号重畳回路
- 13 … フィールドメモリ
- 15 … R / W 制御器
- 19 … 時刻コード抜取回路
- 20 … K s メモリ A
- 21 … K s メモリ B
- 22 … 時刻コード照合回路
- 29 … 乱数発生回路
- 30 … ライン番号への変換回路
- 31 … 符号・課金処理回路
- 32 … C / N 判定回路

代理人 浅 村 皓

第 1 圖



第 2 図



第 3 図

ヘッダの内容例						内容例	
b ₀	b ₁	b ₂	b ₃	b ₄	b ₅		
0	0	0	0	0	0	単独	KS パケット No. 1
1	0	0	0	0	0	複数	KS パケット No. 2
0	1	0	0	0	0	複数	KS パケット No. 3
1	1	0	0	0	0	複数	KS パケット No. 4
0	0	1	0	0	0	複数	KS パケット No. 5
1	0	1	0	0	0	複数	KS パケット No. 6
0	1	1	0	0	0	複数	KS パケット No. 7

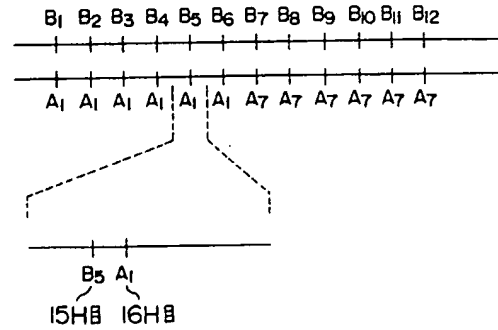
第 4 図

分 秒				KS
X	X	1	0	KS10
X	X	2	0	KS20
X	X	3	0	KS30
X	X	4	0	KS40
X	X	5	0	KS50
X	*	0	0	KS00

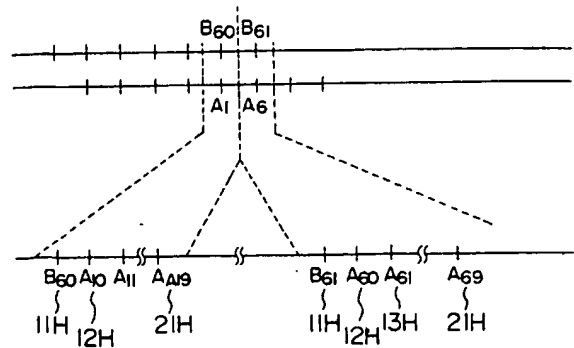
第 5 図

分 秒				KS
X	X	5	0	KS50
X	*	0	0	KS00
X	*	1	0	KS10'
X	*	2	0	KS20'
X	*	3	0	KS30'
X	*	4	0	KS40'

第 6 図



第 7 図



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.